# PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-241290**
(43)Date of publication of application : **11.09.1998**

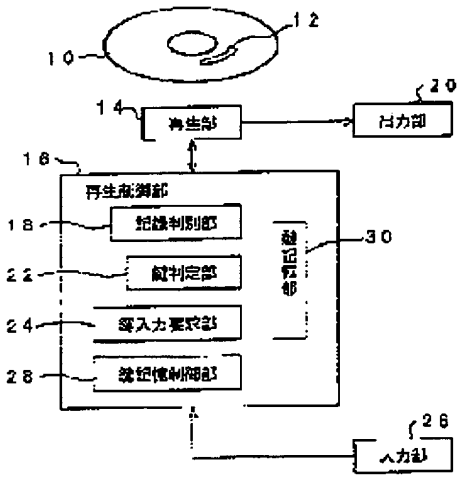
(51)Int.Cl. **G11B 20/10**
**G06F 9/06**
**G06F 12/14**

(21)Application number : **09-055518**
(22)Date of filing : **24.02.1997**

(71)Applicant : **VICTOR CO OF JAPAN LTD**
(72)Inventor : **MOCHIZUKI MASAKI**

## (54) INFORMATION REPRODUCING METHOD AND DEVICE THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information reproducing method capable of improving operability by simplifying the management of cryptographic keys without incurring the lowering of security and device therefor.
SOLUTION: When a disk 10 is reproduced at first, the inputting of a cryptographic key is requested by a key input requesting part 2A. A user inputs a cryptographic key with an input part 26. When it is judged to be correct cryptographic key by a key judging part 22, the cryptographic key is stored in a key storage part 30 by a key storage control part 28. At the time of a next reproduction, when it is discriminated that cryptographic key corresponding to the disk is stored in the key storage part 30 by the key judging part 2, in a reproduction control part 16, the stored cryptographic key is automatically read out and whether the cryptographic key is correct or not is judged in the key judging part 22. When the cryptographic key is judged to be correct, the reproducing of corresponding information is performed.




LEGAL STATUS

| | |
|---|---|
| [Date of request for examination] | 28.03.2003 |
| [Date of sending the examiner's decision of rejection] | |
| [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration] | |
| [Date of final disposal for application] | |
| [Patent number] | 3704868 |
| [Date of registration] | 05.08.2005 |
| [Number of appeal against examiner's decision of rejection] | |
| [Date of requesting appeal against examiner's decision of rejection] | |
| [Date of extinction of right] | |

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－241290

(43)公開日　平成10年(1998)９月11日

| (51)Int.Cl.[6] | 識別記号 | ＦＩ | |
|---|---|---|---|
| Ｇ１１Ｂ　20/10 | | Ｇ１１Ｂ　20/10 | Ｈ |
| Ｇ０６Ｆ　9/06 | ５５０ | Ｇ０６Ｆ　9/06 | ５５０Ｇ |
| 12/14 | ３２０ | 12/14 | ３２０Ｆ |

審査請求　未請求　請求項の数８　ＦＤ　（全 12 頁）

(21)出願番号　特願平9－55518

(22)出願日　平成９年(1997)２月24日

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地

(72)発明者　望月　聖樹
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

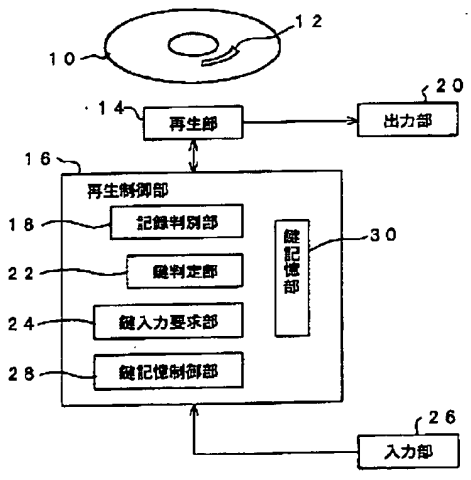
(74)代理人　弁理士　梶原　康稔

(54)【発明の名称】　情報再生方法及び装置

(57)【要約】

【課題】　セキュリティの低下を招くことなく、暗号鍵の管理を簡略化して使い勝手の向上を図ることができる情報再生方法及びその装置を提供する。

【解決手段】　最初にディスク１０が再生されるときに、鍵入力要求部２４によって暗号鍵の入力が要求される。利用者は、入力部２６で暗号鍵を入力する。鍵判定部２２によって正しい暗号鍵であると判定されたときは、鍵記憶制御部２８によって暗号鍵が鍵記憶部３０に記憶される。次の再生時には、鍵判別部２２でディスクに対応した暗号鍵が鍵記憶部３０に記憶されていると判別されると、再生制御部１６では、鍵記憶部３０から記憶されている暗号鍵が自動的に読み出され、鍵判別部２２でその暗号鍵が正しいかどうかが判別される。暗号鍵が正しい場合には、対応する情報の再生が行われる。



1

【特許請求の範囲】

【請求項１】　暗号鍵が入力されたときに、その暗号鍵に基づいて対応する媒体の情報を再生する情報再生方法において、

入力された正しい暗号鍵を記憶するステップ；情報再生の際に、前記記憶された暗号鍵に基づいて対応する情報を再生するステップ；を備えたことを特徴とする情報再生方法。

【請求項２】　暗号鍵が入力されたときに、その暗号鍵に基づいて対応する媒体の情報を再生する情報再生方法において、

入力された正しい暗号鍵を記憶するステップ；暗号鍵を呼び出すための呼出鍵を設定して記憶するステップ；情報再生の際に、前記記憶された呼出鍵が入力されたときは、前記記憶されている暗号鍵に基づいて対応する情報を再生するステップ；を備えたことを特徴とする情報再生方法。

【請求項３】　暗号鍵が入力されたときに、その暗号鍵に基づいて対応する媒体の情報を再生する情報再生方法において、

入力された正しい暗号鍵を記憶するステップ；正しい暗号鍵を簡略化して簡略鍵を生成し記憶するステップ；情報再生の際に、前記記憶された簡略鍵が入力されたときは、前記記憶されている暗号鍵に基づいて対応する情報を再生するステップ；を備えたことを特徴とする情報再生方法。

【請求項４】　前記媒体は、ディスクＩＤが記録されたディスク媒体であり、前記暗号鍵は、前記ディスクＩＤに対応して設定されたことを特徴とする請求項１，２又は３のいずれかに記載の情報再生方法。

【請求項５】　暗号鍵が入力されたときに、その暗号鍵に基づいて対応する媒体の情報を再生する情報再生装置において、

鍵情報を入力する入力手段；媒体の情報を再生する再生手段；前記入力手段によって入力された正しい暗号鍵を記憶する記憶手段；情報再生の際に、前記記憶手段に記憶された暗号鍵に基づいて、対応する情報を前記再生手段で再生する再生制御手段；を備えたことを特徴とする情報再生装置。

【請求項６】　暗号鍵が入力されたときに、その暗号鍵に基づいて対応する媒体の情報を再生する情報再生装置において、

鍵情報を入力する入力手段；媒体の情報を再生する再生手段；前記入力手段で入力された正しい暗号鍵を記憶する第１の記憶手段；暗号鍵を呼び出すための呼出鍵を設定する呼出鍵設定手段；これによって設定された呼出鍵を記憶する第２の記憶手段；情報再生の際に、前記第２の記憶手段に記憶された呼出鍵が前記入力手段によって入力されたときは、前記第１の記憶手段に記憶されている暗号鍵に基づいて、対応する情報を前記再生手段で再生する再生制御手段；を備えたことを特徴とする情報再生装置。

2

【請求項７】　暗号鍵が入力されたときに、その暗号鍵に基づいて対応する媒体の情報を再生する情報再生装置において、

鍵情報を入力する入力手段；媒体の情報を再生する再生手段；前記入力手段で入力された正しい暗号鍵を記憶する第１の記憶手段；暗号鍵を簡略化して簡略鍵を生成する簡略鍵生成手段；これによって生成された簡略鍵を記憶する第２の記憶手段；情報再生の際に、前記第２の記憶手段に記憶された簡略鍵が前記入力手段によって入力されたときは、前記第１の記憶手段に記憶されている暗号鍵に基づいて、対応する情報を前記再生手段で再生する再生制御手段；を備えたことを特徴とする情報再生装置。

【請求項８】　前記媒体は、ディスクＩＤが記録されたディスク媒体であり、前記暗号鍵は、前記ディスクＩＤに対応して設定されたことを特徴とする請求項５，６又は７のいずれかに記載の情報再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、暗号鍵を利用した情報再生方法及びその装置にかかり、更に具体的には、その暗号鍵の管理技術の改良に関する。

【０００２】

【背景技術】よく知られているように、ＣＤなどのディスクパッケージメディアでは、ディスクに含まれる情報が全てディスク所有者に開示される。従って、ディスク所有者は、そのディスクを入手した時点でディスクに含まれる全ての情報を利用することができる。このため、ディスクの価格は、そのディスクに含まれている全ての情報に対して設定され、消費者は設定された価格を支払ってディスクを購入するという流通形態となっている。これは、ディスクに含まれる情報の「所有」に対して対価を支払うという考え方である。

【０００３】一般的に、ディスクそのものは極めて安価に製造できる。このため、ディスクに対して支払われる価格は、ほとんどディスクに含まれている情報の質と量に対するものであると考えることができる。「所有」に対価を支払う流通システムでは、ディスク内の情報の全てを必要としない場合にも、そのディスクを入手するためにはディスクに含まれる全ての情報に対して料金を支払わなくてはならない。別言すれば、価格にふさわしい情報の質と量を満たすためには、様々な消費者の要求を満たすように、情報の内容を若干変えただけの多種多様なディスクを製造しなければならない。このような流通システムは、消費者にとって不都合なだけではなく、生産者にとってもコストアップや流通の複雑さを生む要因となる。

【０００４】これに対し、情報の「所有」ではなく、情

報の「利用」に対して対価を支払う流通形態として「超流通システム」が考えられている。このシステムによれば、消費者は、利用した情報に対してのみ対価を支払えばよく、上述した情報の「所有」に料金を支払う流通システムの不都合を解消でき、より合理的なシステムであると考えられる。この超流通システムでは、情報の利用状況や利用制限情報が、通信ネットワークを介して管理システムと授受される。

【０００５】図６には、そのような超流通システムの一例が示されている。この例は、ゲームソフトに適用した例である。ゲームソフトが記録されたディスク９００は、例えばゲーム雑誌９０２に付録として添付されている。ゲームソフトの利用者は、ゲーム雑誌９０２を購入することでディスク９００を入手する（矢印ＦＡ参照）。

【０００６】ディスク９００には、ディスク毎の固有のＩＤが記録されている。例えば、米国特許第５４００３１９号には、光ディスクの作製後に、光ディスク本来の記録密度よりはるかに低密度の情報を情報記録面上に記録する方法が開示されている。低密度情報の記録は、強力なレーザ光線などを照射して光ディスク基板や基板上の反射膜を永久変形させることで行われる。

【０００７】一方、ディスク９００が再生されるパソコン（あるいはプレーヤ）９０４には、コネクタや通信ポートが設けられており、それぞれＩＣカード９０６やモデム９０８が接続されている。ＩＣカード９０６には、ゲームソフトの再生限度額データが予め記憶されており、このデータはゲームソフトの再生毎に減額される。モデム９０８は通信路を通じてゲームソフト供給者の管理用コンピュータ９１０に接続される。管理用コンピュータ９１０では、再生枠の設定や再生料金の回収が行われる。

【０００８】例えば、使用者は、パソコン９０４にディスク９００をセットする。そして、①ディスクのＩＤやドライブNO.，②再生したいゲームソフトのＩＤ，③再生装置であるパソコンのＩＤ，④ＩＣカードのＩＤなどの情報がパソコン９０４によって管理用コンピュータ９１０に送られる（矢印ＦＢ参照）。管理用コンピュータ９１０では、転送された情報を組み合わせて、暗号鍵（ないしは暗証番号）を生成転送する（矢印ＦＣ参照）。最も簡単な例を示すと、ディスクのＩＤが「１２３」，ドライブ番号が「１２２」，使用したいゲームソフトのタイトルキーが「６６６」の場合、暗号鍵を「４２１」とする。パソコン９０４では、ディスクのＩＤ「１２３」，ドライブ番号「１２２」と使用者が入力する暗号鍵「４２１」が加算される。すると、合計が「６６６」となり、これが再生すべきタイトルキーである。パソコン９０４では、このタイトルキー「６６６」のゲームソフトが再生されるという具合である。

【０００９】このように、使用者は、ディスクの再生前



に一度ソフト供給側に連絡し、必要とする情報を利用するための暗号鍵を入手する。そして、この暗号鍵を利用して情報を利用する。本例では、ディスク９００に格納されている多数のゲームソフトのうち、暗号鍵に該当するものが再生される。情報利用の対価は、ＩＣカード９０６に予め記憶されている金額から減算される。利用者は、ＩＣカード９０６の再生限度額の範囲で、ゲームソフトを楽しむことができる。

【００１０】このようなシステムによれば、ディスクがあっても暗号鍵がなければその情報を利用することができないので、ディスクの不正コピー自体が意味を持たなくなり、その防止を図ることができる。また、暗号鍵の生成にディスク固有のＩＤを利用しているため、ディスク毎の暗号鍵を設定することができ、暗号鍵の使い回しといった不正も不可能になる。

【００１１】

【発明が解決しようとする課題】しかしながら、上述した手法によれば、ディスク一枚毎に異なる暗号鍵が設定されるため、利用者側ではそれらの暗号鍵の管理が必要となる。特に、ディスクが多数存在するような場合には、その管理に相当の手数がかかる。すなわち、ディスクを再生する度に暗号鍵を入力しなければならない。また、ディスクを交換したときは、異なる暗号鍵を入力しなければならない。暗号鍵を忘れてしまったような場合には、その付与のための手続を再度行わなければならない。従って、情報提供者からみると、その不正に対するセキュリティが高まって非常に好都合であるが、情報利用者からみると情報を利用する度に暗号鍵が必要となり、必ずしも使い勝手がよいとは言えない。

【００１２】この発明は、以上の点に着目したもので、セキュリティの低下を招くことなく、その管理を簡略化して使い勝手の向上を図ることができる情報再生方法及びその装置を提供することを、その目的とするものである。

【００１３】

【課題を解決するための手段】前記目的を達成するため、この発明の情報再生方法は、暗号鍵が入力されたときに、その暗号鍵に基づいて対応する媒体の情報を再生する情報再生方法において、入力された正しい暗号鍵を記憶するステップ（S18, S20, S22, S24, S26, S26）；情報再生の際に、前記記憶された暗号鍵に基づいて対応する情報を再生するステップ（S16, S30, S32, S28）；を備えたことを特徴とする。これに対応する情報再生装置は、暗号鍵が入力されたときに、その暗号鍵に基づいて対応する媒体の情報を再生する情報再生装置において、鍵情報を入力する入力手段（24, 26）；媒体の情報を再生する再生手段（14, 20）；前記入力手段によって入力された正しい暗号鍵を記憶する記憶手段（22, 30, 28）；情報再生の際に、前記記憶手段に記憶された暗号鍵に基づいて、対応する情報を前記再生手段で再生する再生制御手

段（22）；を備えたことを特徴とする。

【００１４】他の情報再生方法は、入力された正しい暗号鍵を記憶するステップ；暗号鍵を呼び出すための呼出鍵を設定して記憶するステップ（S40, S42, S44, S46）；情報再生の際に、前記記憶された呼出鍵が入力されたときは、前記記憶されている暗号鍵に基づいて対応する情報を再生するステップ（S48, S50, S52, S54, S56, S30, S32, S28）；を備えたことを特徴とする。対応する情報再生装置は、鍵情報を入力する入力手段；媒体の情報を再生する再生手段；前記入力手段で入力された正しい暗号鍵を記憶する第１の記憶手段（28, 30）；暗号鍵を呼び出すための呼出鍵を設定する呼出鍵設定手段（24, 26, 28）；これによって設定された呼出鍵を記憶する第２の記憶手段（28, 30）；情報再生の際に、前記第２の記憶手段に記憶された呼出鍵が前記入力手段によって入力されたときは、前記第１の記憶手段に記憶されている暗号鍵に基づいて、対応する情報を前記再生手段で再生する再生制御手段（16, 22）；を備えたことを特徴とする。

【００１５】更に他の情報再生方法は、入力された正しい暗号鍵を記憶するステップ；正しい暗号鍵を簡略化して簡略鍵を生成し記憶するステップ（S60, S62, S64, S66, S68, S70）；情報再生の際に、前記記憶された簡略鍵が入力されたときは、前記記憶されている暗号鍵に基づいて対応する情報を再生するステップ（S48A, S50A, S52A, S54A, S56A, S30, S32, S28）；を備えたことを特徴とする。対応する情報再生装置は、鍵情報を入力する入力手段；媒体の情報を再生する再生手段；前記入力手段で入力された正しい暗号鍵を記憶する第１の記憶手段；暗号鍵を簡略化して簡略鍵を生成する簡略鍵生成手段（32）；これによって生成された簡略鍵を記憶する第２の記憶手段（28, 30）；情報再生の際に、前記第２の記憶手段に記憶された簡略鍵が前記入力手段によって入力されたときは、前記第１の記憶手段に記憶されている暗号鍵に基づいて、対応する情報を前記再生手段で再生する再生制御手段（16, 22）；を備えたことを特徴とする。

【００１６】主要な形態の一つは、情報が記録された記録媒体から情報を読み出す際、特定のアルゴリズムに基づいて生成された暗号の入力を要求する情報再生方法において、情報が記録された記録媒体（10）を他の記録媒体から識別する固有の情報を、前記記録媒体から読み出すステップ（S10, S14）と、前記暗号が入力された際に、それが正しいものであった場合には前記記録媒体固有の情報と組み合わせて再生装置に記憶するステップ（S16, S18, S20, S22, S24, S26）と、前記暗号入力要求動作移行時に、前記記録媒体固有の情報と組み合わせて再生装置に記憶された前記暗号が存在するか否かを判別するステップ（S16）とを有し、前記記録媒体固有の情報と組み合わせて再生装置に記憶された前記暗号が存在する場合には、前記暗号入力要求動作をスキップして前記記憶された暗号が正しいものかどうかを判断するステップ（S16, S30, S32）に移行することを特徴とする。



【００１７】他の形態の情報再生方法は、情報が記録された記録媒体をほかの記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、前記暗号が入力された際に、それが正しいものであった場合には前記記録媒体固有の情報と組み合わせて再生装置に記憶するステップと、前記暗号入力要求動作移行時に、前記記録媒体固有の情報と組み合わせて再生装置に記憶された前記暗号が存在するか否かを判別するステップと、前記記録媒体固有の情報と組み合わせて再生装置に記憶された前記暗号が存在する場合には、前記再生装置に記憶された暗号を読み出すための別の識別文入力を要求するステップ（S18）とを有し、前記別の識別文が正しいものであった場合には前記再生装置に記憶された暗号を読み出し、前記暗号入力要求動作をスキップして前記記憶された暗号が正しいものかどうかを判断するステップ（S48, S50, S52, S54, S56, S30, S32）に移行することを特徴とする。

【００１８】更に他の形態の情報再生方法は、情報が記録された記録媒体をほかの記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、前記暗号が入力された際にそれが正しいものであった場合には、前記暗号を所定のアルゴリズムで簡略化した暗号情報に変換するステップ（S40, S42, S44）と、前記記録媒体固有の情報と前記暗号情報と前記簡略化された暗号情報を組み合わせて再生装置に記憶するステップ（S46）と、前記暗号入力要求動作移行時に、前記記録媒体固有の情報と組み合わせて再生装置に記憶された前記暗号が存在するか否かを判別するステップとを有し、前記記録媒体固有の情報と組み合わせて再生装置に記憶された前記暗号が存在する場合には、それらと組み合わせて再生装置に記憶された前記簡略化された暗号情報を基に情報再生の制御を行うことを特徴とする。

【００１９】更に他の形態によれば、前記媒体は、ＢＣＡ（Burst Cutting Area）にディスクＩＤが記録されたＤＶＤであり、前記暗号鍵は、前記ディスクＩＤに対応して設定されたことを特徴とする。

【００２０】この発明の前記及び他の目的，特徴，利点は、以下の詳細な説明及び添付図面から明瞭になろう。

【００２１】

【発明の実施の形態】以下、発明の実施の形態について、実施例を参照しながら詳細に説明する。

【実施例１】まず、図１及び図２を参照して本発明の実施例１を説明する。図１には実施例１の情報再生方法がフローチャートとして示されており、図２には実施例１の情報再生装置の構成がブロック図として示されている。これらの図において、光ディスク１０は、例えばＤＶＤ規格に対応したディスクであり、映画やゲームソフトなどの主情報が記録されている領域とは異なる固有情報領域１２に各種の情報が記録されている。例えば、デ

ィスクＩＤ，暗号鍵情報，再生制限情報，使用者の個人情報などの情報再生の制御に用いられる情報のうちの一つ以上が記録されている。これらの再生制御情報は、ディスク毎に異なる。

【００２２】なお、ディスク１０に記録されている主情報には、暗号鍵なしで再生可能な情報と、暗号鍵がなければ再生不可能な情報が記録されているものとする。また、初期状態（暗号鍵入力前の状態）で再生制限されている主情報の再生に必要な暗号鍵は、ソフト供給者に対する所定の手続によって予め取得されているものとする。前記固有情報領域１２は、例えば、ディスク１０の情報記録面上，再生読出面上，あるいはそれらに隣接する場所に設定されている。そして、ディスク本来の主情報の記録密度の１／１０から１／１０００の線記録密度の低密度の情報として、固有情報が記録されている。

【００２３】(1) 最初の再生動作

ディスク１０が再生部１４にセットされると、再生制御部１６によってその固有情報領域１２が再生される。そして、記録判別部１８で固有情報がないと判別さたときは（図１ステップＳ１０のN）、再生にあたって暗号鍵が必要とされないディスクであると判断し、再生部１４によって通常の再生が行われる（ステップＳ１２）。再生情報は、出力部２０において再生出力される。

【００２４】他方、記録判別部１８で、固有情報領域１２に固有情報が記録されていると判別されたときは（ステップＳ１０のY）、ディスク固有情報，すなわち、暗号鍵情報，ディスク識別情報，再生許可タイトル，個人情報などが読み取られる（ステップＳ１４）。そして、これらの固有情報中に、そのディスクに対応した暗号鍵が記憶されているかどうかが、鍵判定部２２で判定される（ステップＳ１６）。ディスク１０を初めて再生するときは、上述したように暗号鍵は利用者が入力する。従って、暗号鍵は、固有情報として記憶されていない。このため、鍵判定部２２では、暗号鍵がないと判定され（ステップＳ１６のN）、暗号鍵の入力要求が行われる（ステップＳ１８，ステップＳ２０のN）。すなわち、鍵入力要求部２４によって、その旨が出力部２０に音声あるいは映像として出力される。なお、このとき、ディスク１０の非制限情報を再生してもよい（ステップＳ１７）。利用者が暗号鍵の入力をキャンセルしたときも同様である（ステップＳ２１）。

【００２５】利用者が、入力要求に基づいて入力部２６により暗号鍵を入力したとすると（ステップＳ２０のY）、鍵判定部２２でその適否が判定される（ステップＳ２２）。その結果、暗号鍵が適切なものであると判定されたときは（ステップＳ２２のY）、その記憶の有無が利用者に問われる（ステップＳ２４）。すなわち、鍵記憶制御部２８によってその旨が出力部２０に音声あるいは映像として出力される。利用者が、入力部２６により暗号鍵の記憶を要求する旨を通知したときは（ステップＳ２４のY）、鍵記憶部３０にディスク１０の固有情報と組み合わせて暗号鍵を記憶する（ステップＳ２６）。そして、その後、入力された暗号鍵に対応する主情報が再生される（ステップＳ２８）。なお、利用者が暗号鍵の記憶を要求しなかったときには（ステップＳ２４のN）、そのまま主情報が再生される（ステップＳ２８）。



【００２６】(2) ２回目以降の再生動作

次に、以上のようにして暗号鍵が記憶された再生装置で、ディスクを再生する場合の動作について説明する。再生装置では、上述したようにしてディスク１０の固有情報領域１２から固有の情報が読み出される（ステップＳ１４）。次に、ステップＳ１６において、鍵判別部２２でディスクに対応した暗号鍵が記憶されていると判別される（ステップＳ１６のY）。すると、再生制御部１６では、鍵記憶部３０から記憶されている暗号鍵が自動的に読み出され（ステップＳ３０）、鍵判別部２２でその暗号鍵が正しいかどうかが判別される（ステップＳ３２）。その結果、読み出された暗号鍵が正しくない場合には（ステップＳ３２のN）、上述したように暗号鍵の入力が要求される（ステップＳ１８）。例えば、ディスクが、暗号鍵を記憶したときに再生したディスクと異なるような場合が該当する。一方、暗号鍵が正しい場合には（ステップＳ３２のY）、対応する情報の再生が行われる（ステップＳ２８）。

【００２７】このように、本実施例によれば、再生装置では、ディスクの再生に際して、ディスクの固有情報と暗号鍵情報の有無や、暗号鍵情報の正否によって再生情報の範囲が決定される。最初は、適正な暗号鍵が入力されて制限がはずされ、再生動作が行われるとともにその暗号鍵が記憶される。同じディスクを同じ再生装置で再生するときは、記録された暗号鍵に基づいて制限がはずされ、再生動作が行われる。すなわち、最初に暗号鍵を用いて再生動作を行う際に暗号鍵を記憶させておけば、再びそのディスクを再生するときは、記憶された暗号鍵を用いて制限が解除されて再生動作が行われる。従って、利用者は、暗号鍵をディスクの再生動作毎に入力する手間から開放され、暗号鍵の管理が簡略化されて使い勝手が向上する。

【００２８】

【実施例２】次に、図３を参照しながら実施例２について説明する。この実施例は、一度暗号鍵が入力記憶されたディスクを再生する場合に、その記憶された暗号鍵を呼び出すための別の鍵ないしは暗証番号を再生装置側で設定するようにしたものである。セキュリティを高めるためには、暗号鍵は複雑なもののほうがよい。しかし、ディスク再生の度に複雑な暗号鍵を入力するのは、利用者にとって非常に負担である。しかし、仮に暗号鍵の入力の負担を軽減する適当な方法があれば、高度なセキュリティを持つ複雑な暗号鍵を使用することができるの

で、好都合である。そこで、本実施例では、ソフト供給者から暗号鍵を受け取って最初に情報再生を行う際には複雑な暗号鍵の入力が必要であるが、次の再生からは簡単な暗号（以下「呼出鍵」という）の入力で済むようになっている。

【００２９】図３には実施例２の情報再生方法のフローチャートが示されている。本実施例の再生装置のブロック構成は実施例１に対応しており、各部では暗号鍵の他に呼出鍵も処理の対象となっている。なお、上述した実施例１と対応するものには同一の符号を用いる。本実施例では、再生制御部１６の鍵記憶部３０に、暗号鍵を記憶する領域と、それを呼び出すための別の簡略な暗号鍵である呼出鍵を記憶する領域が設けられている。なお、呼出鍵としては、簡単に暗証できるような数字，文字，記号，あるいはそれらの組み合わせが用いられる。呼出鍵は、どのディスクに対しても共通に設定してよいし、もちろん異なるものに設定してもよい。

【００３０】(1) 最初の再生動作

ディスク１０のセットから、固有情報の読取り（ステップＳ１０，Ｓ１４），通常再生（ステップＳ１２），暗号鍵のチェック（ステップＳ１６），非制限情報の再生（ステップＳ１７，Ｓ２１），暗号鍵の入力要求（ステップＳ１８），入力チェック（ステップＳ２０，Ｓ２２），暗号鍵記憶の問合せ（ステップＳ２４）については、上述した実施例と同様である。

【００３１】本実施例では、暗号鍵記憶時に、それを呼び出すための呼出鍵の設定の有無が利用者に問われる（ステップＳ４０）。すなわち、鍵記憶制御部２８によってその旨が出力部２０に音声あるいは映像として出力される。利用者が、入力部２６により呼出鍵の設定を要求する旨を通知したときは（ステップＳ４０のＹ）、鍵記憶制御部２８によって呼出鍵を設定する旨が出力部２０で出力され、利用者は、入力部２６によって呼出鍵を設定入力する（ステップＳ４２）。そして、設定が終了した時点で（ステップＳ４４のＹ）、鍵記憶制御部２８によって、鍵記憶部３０にディスク１０の固有情報及び暗号鍵と組み合わせて呼出鍵を記憶する（ステップＳ４６）。その後、入力された暗号鍵に対応する主情報が再生される（ステップＳ２８）。なお、利用者が呼出鍵の設定を要求しなかったときには（ステップＳ４０のＮ）、鍵記憶部３０にディスク１０の固有情報及び暗号鍵を組み合わせて記憶し（ステップＳ４１）、その後主情報が再生される（ステップＳ２８）。

【００３２】(2) ２回目以降の再生動作

次に、以上のようにして暗号鍵が記憶されるとともに、その呼出鍵が設定された再生装置で、ディスクを再生する場合の動作について説明する。なお、暗号鍵のみが記憶されており、呼出鍵が設定されなかった場合の動作は、前記実施例１と同様である（ステップＳ４８のＮ）。



【００３３】この場合、上述した最初の動作で暗号鍵及び呼出鍵が記録されている。このため、再生装置では、鍵判別部２２でディスクに対応した暗号鍵が記憶されていると判別される（ステップＳ１６のＹ）。続いて、鍵判別部２２で暗号鍵に対応した呼出鍵が記憶されていると判別される（ステップＳ４８のＹ）。すると、再生制御部１６では、鍵記憶部３０から記憶されている呼出鍵が自動的に読み出され（ステップＳ５０）、更に呼出鍵の入力要求が行われる（ステップＳ５２）。すなわち、鍵入力要求部２４によって、その旨が出力部２０に音声あるいは映像として出力される。

【００３４】利用者が、入力要求に基づいて入力部２６により呼出鍵を入力したとすると（ステップＳ５４のＹ）、鍵判定部２２でその適否が判定される（ステップＳ５６）。その結果、呼出鍵が適切なものであると判定されたときは（ステップＳ５６のＹ）、鍵記憶部３０から記憶されている暗号鍵が自動的に読み出され（ステップＳ３０）、鍵判別部２２でその暗号鍵が正しいかどうかが判別される（ステップＳ３２）。その結果、読み出された暗号鍵が正しくない場合には（ステップＳ３２のＮ）、上述したように暗号鍵の入力が要求される（ステップＳ１８）。一方、暗号鍵が正しい場合には（ステップＳ３２のＹ）、対応する情報の再生が行われる（ステップＳ２８）。

【００３５】このように、本実施例によれば、最初の再生時に、利用者によって呼出鍵が設定され、対応する暗号鍵とともに記憶される。次回の再生時には、呼出鍵がチェックされ、これが適正に入力されたときは自動的に暗号鍵情報が呼び出される。そして、この暗号鍵を利用して制限が解除され、主情報が再生される。このため、利用者は、最初を除けば、簡単な呼出鍵を管理するのみでよく、鍵管理の負担が軽減される。呼出鍵の設定は、ソフト供給側から提示された暗号鍵を擬似的に利用者側で再設定することになり、ソフト供給者のシステムに対する秘匿性の要求と、利用者の簡便性とが両立するようになる。

【００３６】

【実施例３】次に、図４及び図５を参照しながら実施例３について説明する。図４は実施例３のフローチャート，図５は実施例３のブロック図である。この実施例は、暗号鍵そのものを再生装置側で簡略化して簡略鍵を生成し、これを上述した呼出鍵として使用することで、鍵入力の負担を軽減するようにしたものである。ソフト供給者から暗号鍵を受け取って最初の情報再生を行う際には、複雑な暗号鍵の入力が必要であるが、次の再生からは簡単な簡略鍵の入力で済む。再生装置側には、暗号鍵を簡略化するためのアルゴリズムが用意される。具体的には、図５にブロック図を示すように、鍵簡略処理部３２によって、暗号鍵を簡略化するためのアルゴリズムに基づく簡略化の処理が行われる構成となっている。

【００３７】（1）最初の再生動作

ディスク１０のセットから、固有情報の読取り（ステップＳ１０，Ｓ１４），通常再生（ステップＳ１２），暗号鍵のチェック（ステップＳ１６），非制限情報の再生（ステップＳ１７，Ｓ２１），暗号鍵の入力要求（ステップＳ１８），入力チェック（ステップＳ２０，Ｓ２２），暗号鍵記憶の問合せ（ステップＳ２４）については、上述した実施例と同様である。

【００３８】本実施例では、暗号鍵記憶時に、暗号鍵の簡略化の有無が利用者に問われる（ステップＳ６０）。すなわち、鍵簡略処理部３２によってその旨が出力部２０に音声あるいは映像として出力される。利用者が、入力部２６により暗号鍵の簡略化を要求する旨を通知したときは（ステップＳ６０のＹ）、鍵簡略処理部３２によって暗号鍵の簡略化が実行される（ステップＳ６２）。簡略化は、例えば１６桁の暗号鍵のうち下３桁をそのディスクと再生装置の組み合わせにおける簡略鍵とするというような手法で行われる。これによって生成させた簡略鍵は、出力部２０に出力表示される（ステップＳ６４）。ここで、表示された簡略鍵に問題があると判断したときは（ステップＳ６６のＮ）、利用者はその旨を入力部２６によって入力する。すると、鍵簡略処理部３２では、アルゴリズムを若干代えて再び暗号鍵の簡略化が行われる（ステップＳ６８）。例えば、前回表示した簡略鍵の下一桁の数字を一つ変えるという具合で、再度簡略化が行われる。そして、処理後の簡略鍵が表示される（ステップＳ６４）。

【００３９】利用者は、表示された簡略鍵を検討する。例えば、他のディスクの簡略鍵と異なっているか，あるいは逆に同じ鍵になっているかなどである。特に問題がないと判断したときは（ステップＳ６６のＹ），その旨を入力部２６によって入力する。すると、鍵記憶制御部２８によって、鍵記憶部３０にディスク１０の固有情報，暗号鍵，及び対応する簡略鍵が記憶される（ステップＳ７０）。その後、入力された暗号鍵に対応する主情報が再生される（ステップＳ２８）。なお、利用者が暗号鍵の簡略化を要求しなかったときには（ステップＳ６０のＮ），鍵記憶部３０にディスク１０の固有情報及び暗号鍵を組み合わせて記憶し（ステップＳ４１），その後主情報が再生される（ステップＳ２８）。

【００４０】（2）２回目以降の再生動作

この場合の動作は、前記実施例２とほぼ同様である（ステップＳ４８Ａ～Ｓ５６Ａ参照）。ただし、本実施例では、呼出鍵の代わりに簡略鍵が用いられる。

【００４１】このように、本実施例によれば、最初の再生時に、利用者によって暗号鍵の簡略化が行われ、簡略鍵が対応する暗号鍵とともに記憶される。次回の再生時には、簡略鍵がチェックされ、これが適正に入力されたときは自動的に暗号鍵情報が呼び出される。そして、この暗号鍵を利用して制限が解除され、主情報が再生される。このため、利用者は、最初を除けば簡略鍵を管理するのみでよく、鍵管理の負担が軽減される。暗号鍵の簡略化は、ソフト供給側から提示された暗号鍵を擬似的に利用者側で再設定することになり、本実施例でも、ソフト供給者のシステムに対する秘匿性の要求と、利用者の簡便性とが両立するようになる。



【００４２】このように、本実施例では、暗号鍵が簡略化され、簡略鍵が前記実施例の呼出鍵として使用される。このため、前記実施例と同様に、暗号鍵自体のセキュリティを低下させることなく、再生時の暗号鍵入力の手間を大幅に減らすことができる。

【００４３】なお、前記実施例１において一度暗号鍵を再生装置に記憶させてしまうと、それ以降はディスク利用者以外であっても、そのディスクと再生装置の組み合わせであれば制限無しで情報再生が可能となってしまう。しかし、実施例２又は３のように、本来の利用者が呼出鍵又は簡略鍵を記憶させるようにすれば、その利用者以外の者の利用は制限できる。

【００４４】また、一枚のディスクに複数の暗号鍵が設定されており、入力される暗号鍵によって再生できる情報が変わるような場合がある。例えば、複数人がそれぞれ異なるゲームプログラムを異なる暗号鍵で再生するような場合、同一人であっても、異なるゲームプログラムの再生毎に異なる暗号鍵を設定しているような場合である。このようなときは、実施例１の再生制御方法で暗号鍵を記憶させると、複数の暗号鍵を設定した意味が無くなってしまう。そこで、実施例１でも、その都度暗号鍵を記憶させないようにすればよいが、実施例２や３で示したような簡単な識別文や暗証番号による呼出鍵や簡略鍵を利用し、これらと暗号鍵との対応関係を判別するようにすると便利である。

【００４５】

【他の実施例】この発明には数多くの実施の形態があり、以上の開示に基づいて多様に改変することが可能である。例えば、次のようなものも含まれる。

（1）暗号鍵，呼出鍵，簡略鍵としては、数字，文字，記号，文章など、どのようなものでもよい。また、文字数，桁数も特に限定されるものではない。呼出鍵や簡略鍵を複数設定できるようにしてもよいが、再生装置側の記憶容量節約のためには、これを一つ又は少数個に限定するとよい。

（2）前記実施例では、再生装置側に記憶手段を設け、これに鍵情報を記憶することとしたが、媒体側に記憶するようにしてもよい。

（3）前記実施例で示した暗号鍵，呼出鍵，あるいは簡略鍵を書換可能にしてもよい。必要に応じて鍵を変更することで、鍵管理に柔軟性が生ずる。

（4）本実施例は、例えばＤＶＤのようなディスク媒体が好適な適用例であるが、暗号鍵によって再生の制限が解除されるシステムに対応したものであれば、どのよう

13

な媒体にも適用可能である。また、ＤＶＤの場合は、いわゆるＢＣＡがディスクＩＤなどのディスク固有の情報を記録する領域として好適である。

【００４６】

【発明の効果】以上説明したように、本発明によれば次のような効果がある。

(1) 暗号鍵を記憶することとしたので、セキュリティを高めた複雑な暗号鍵が設定されている場合にも、その入力の手間を省いて鍵管理が簡略化され、使い勝手が向上する。

(2) 複雑な暗号鍵の代わりに利用者側で都合のよい鍵を疑似的に呼出鍵として設定でき、鍵入力の負担が低減される。

(3) 暗号鍵を簡略化した簡略鍵を設定でき、鍵入力の負担が低減される。また、簡略化を再生装置側で行うこととしたので、簡略に手間がかからない。

【図面の簡単な説明】

【図１】実施例１の動作を示すフローチャートである。

【図２】実施例１の再生装置の構成を示すブロック図である。

14

【図３】実施例２の動作を示すフローチャートである。

【図４】実施例３の動作を示すフローチャートである。

【図５】実施例３の再生装置の構成を示すブロック図である。

【図６】超流通システムの一例を示す図である。

【符号の説明】

１０…ディスク

１２…固有情報領域

１４…再生部

１６…再生制御部

１８…記録判別部

２０…出力部

２２…鍵判定部

２４…鍵入力要求部

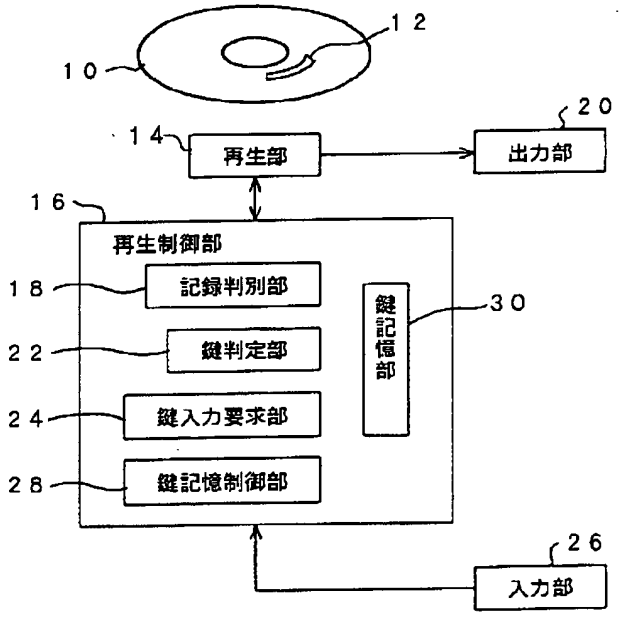
２６…入力部

２８…鍵記憶制御部

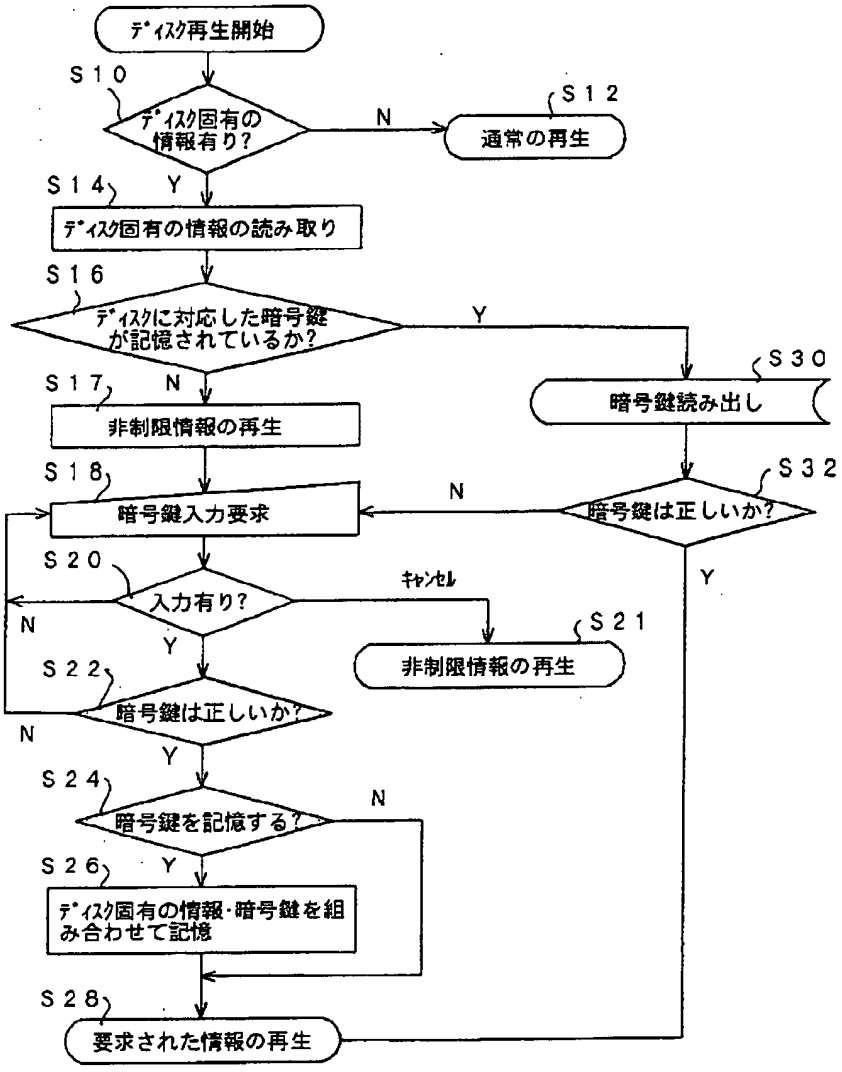
３０…鍵記憶部

３２…鍵簡略処理部

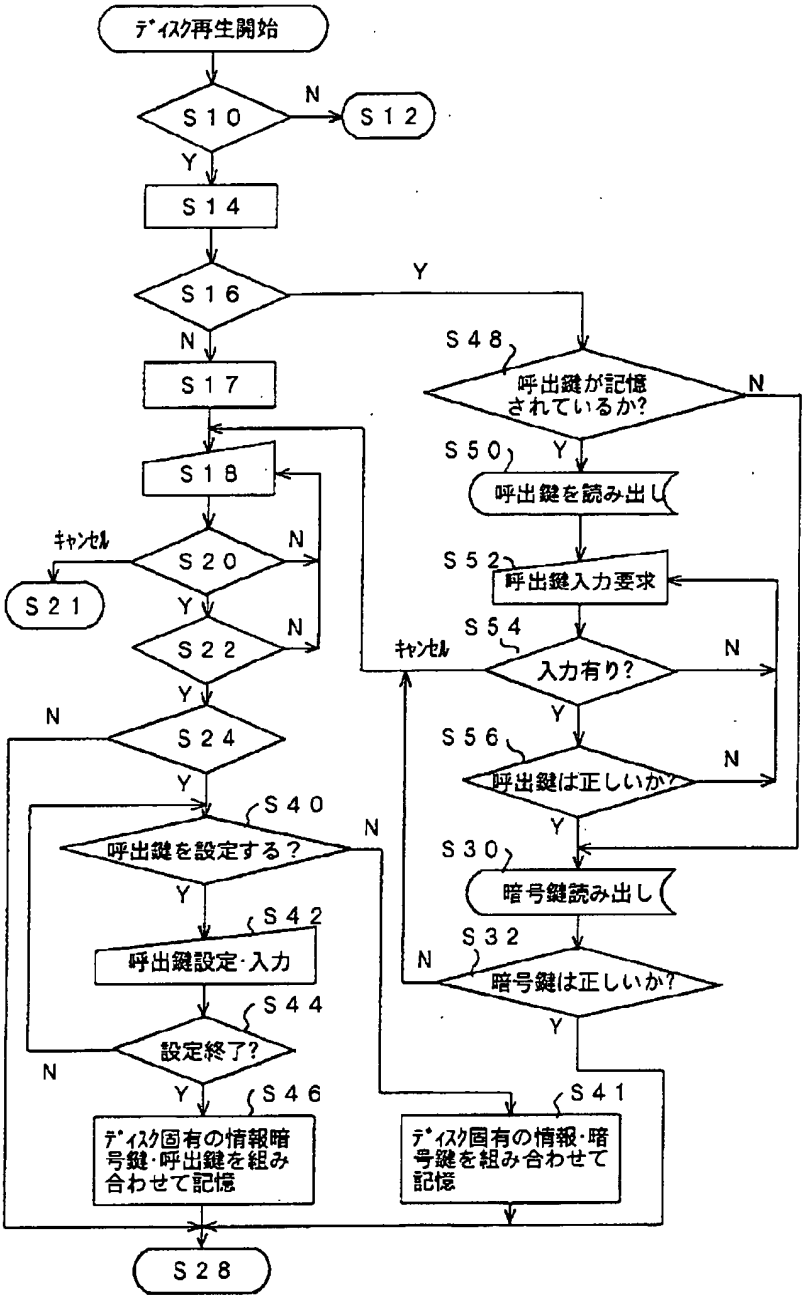
【図２】



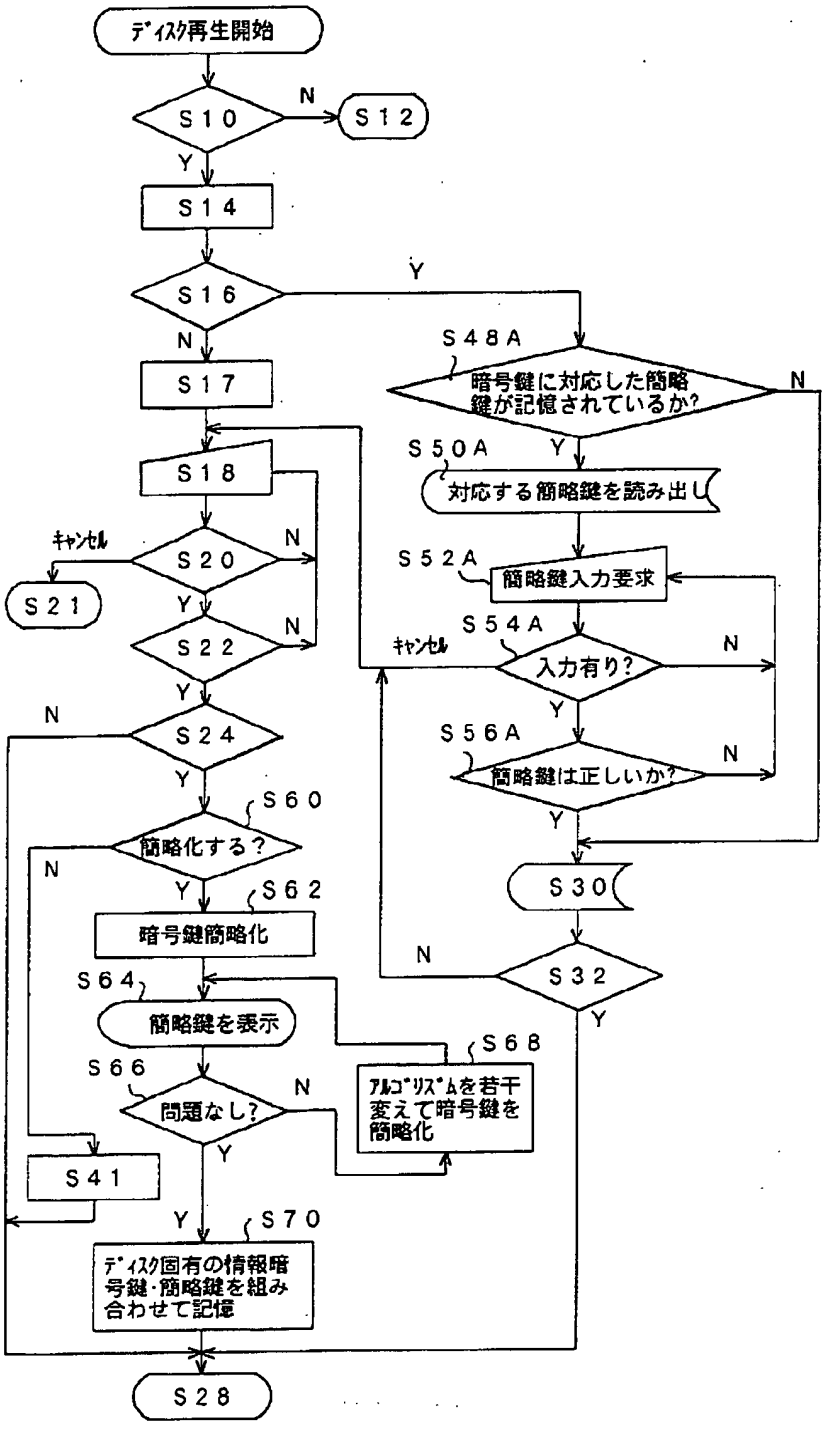
【図１】


ﾃﾞｨｽｸ再生開始
S10
ﾃﾞｨｽｸ固有の情報有り?
N
S12
通常の再生
Y
S14
ﾃﾞｨｽｸ固有の情報の読み取り
S16
ﾃﾞｨｽｸに対応した暗号鍵が記憶されているか?
Y
S30
暗号鍵読み出し
N
S17
非制限情報の再生
S18
暗号鍵入力要求
N
S32
暗号鍵は正しいか?
Y
S20
入力有り?
ｷｬﾝｾﾙ
S21
非制限情報の再生
N
Y
S22
暗号鍵は正しいか?
N
Y
S24
暗号鍵を記憶する?
N
Y
S26
ﾃﾞｨｽｸ固有の情報･暗号鍵を組み合わせて記憶
S28
要求された情報の再生

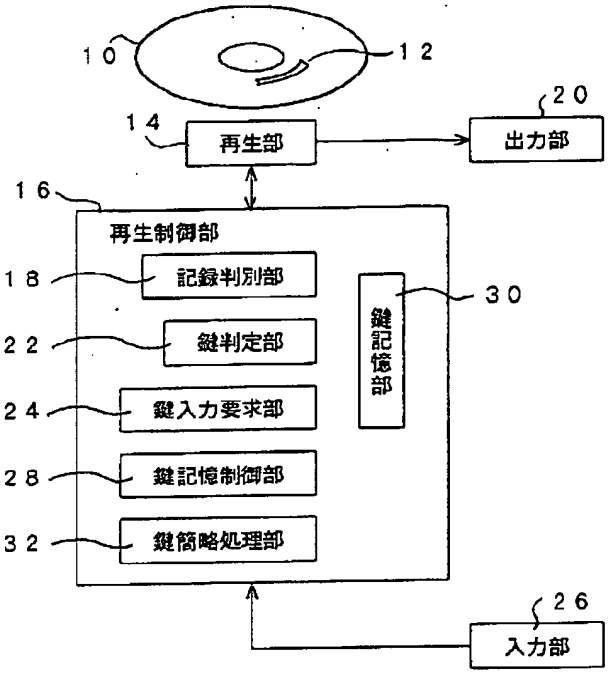
【図３】


ﾃﾞｨｽｸ再生開始
S10
N
S12
Y
S14
S16
Y
N
S17
S18
キャンセル
S20
N
S21
Y
S22
N
Y
S24
N
Y
S40
呼出鍵を設定する？
N
Y
S42
呼出鍵設定･入力
S44
設定終了?
N
Y
S46
ﾃﾞｨｽｸ固有の情報暗号鍵･呼出鍵を組み合わせて記憶
S48
呼出鍵が記憶されているか?
N
Y
S50
呼出鍵を読み出し
S52
呼出鍵入力要求
キャンセル
S54
入力有り?
N
Y
S56
呼出鍵は正しいか?
N
Y
S30
暗号鍵読み出し
S32
N
暗号鍵は正しいか?
Y
S41
ﾃﾞｨｽｸ固有の情報･暗号鍵を組み合わせて記憶
S28

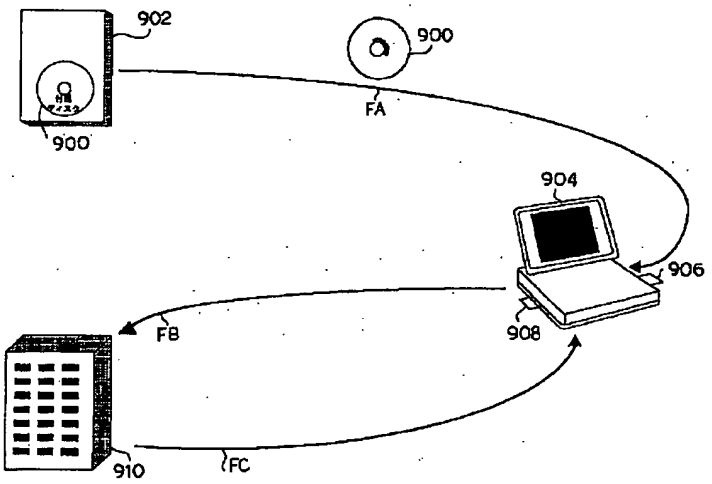
【図４】


ディスク再生開始
S10
N
S12
Y
S14
S16
Y
N
S17
S48A
暗号鍵に対応した簡略鍵が記憶されているか?
N
S18
S50A
Y
対応する簡略鍵を読み出し
キャンセル
S20
N
S21
Y
S52A
簡略鍵入力要求
S22
N
S54A
キャンセル
入力有り?
N
Y
S24
N
S56A
簡略鍵は正しいか?
N
Y
S60
簡略化する?
N
Y
S30
S62
暗号鍵簡略化
N
S32
S64
Y
簡略鍵を表示
S68
S66
問題なし?
N
アルゴリズムを若干変えて暗号鍵を簡略化
Y
S41
Y
S70
ディスク固有の情報暗号鍵・簡略鍵を組み合わせて記憶
S28

【図５】


１０
１２
２０
１４
再生部
出力部
１６
再生制御部
１８
記録判別部
３０
鍵記憶部
２２
鍵判定部
２４
鍵入力要求部
２８
鍵記憶制御部
３２
鍵簡略処理部
２６
入力部

【図６】


902
900
900
FA
904
906
908
FB
910
FC